

Application Serial No. 09/607,375

1. (Currently Amended) A computer-implemented process for authenticating a workstation requesting a network service from a network server via a computer network, comprising the steps:

completing a vulnerability assessment comprising a scan of the workstation to identify at least one of security vulnerabilities that would compromise the secure operation of the workstation on the computer network and evidence of a compromise;

generating workstation security credentials based on the vulnerability assessment, the workstation security credentials comprising one of integrity information describing whether the workstation has been compromised, and security posture information describing the workstation's potential for compromise;

comparing the workstation security credentials to a workstation security policy to determine whether the workstation should be granted access to the network service; and

authorizing access to the network service by the workstation if the workstation security credentials satisfy the workstation security policy, otherwise denying access to the network service by the workstation.

2. (Original) The computer-implemented process recited by Claim 1 further comprising the step of authorizing access to a predetermined level of the network service if the workstation security credentials satisfy a portion of the workstation security policy.

Application Serial No. 09/607,375

3. (Currently Amended) ~~The computer-implemented process recited by Claim 1~~ A computer-implemented process for authenticating a workstation requesting a network service from a network server via a computer network, comprising the steps:

completing a vulnerability assessment of the workstation to identify security vulnerabilities that would compromise the secure operation of the workstation on the computer network;

generating workstation security credentials based on the vulnerability assessment, the workstation security credentials comprising one of integrity information describing whether the workstation has been compromised, and security posture information describing the workstation's potential for compromise, wherein the step of generating the workstation security credentials comprises completing the vulnerability assessment of the workstation by a local workstation assessment service maintained on the workstation, the local workstation assessment service operative to generate the workstation security credentials;

comparing the workstation security credentials to a workstation security policy to determine whether the workstation should be granted access to the network service; and

authorizing access to the network service by the workstation if the workstation security credentials satisfy the workstation security policy, otherwise denying access to the network service by the workstation.

4. (Original) The computer-implemented process recited by Claim 3, wherein the workstation security policy is maintained on the workstation, the process further comprising the step of providing the workstation security credentials from the local workstation assessment service to the workstation security policy.

5. (Cancelled)

[The Remainder of this page has been intentionally left blank.]

Application Serial No. 09/607,375

6. (Currently Amended) ~~The computer-implemented process recited by Claim 5~~ A computer-implemented process for authenticating a workstation requesting a network service from a network server via a computer network, comprising the steps:

completing a vulnerability assessment of the workstation to identify security vulnerabilities that would compromise the secure operation of the workstation on the computer network;

generating workstation security credentials based on the vulnerability assessment, the workstation security credentials comprising one of integrity information describing whether the workstation has been compromised, and security posture information describing the workstation's potential for compromise, wherein the step of generating the workstation security credentials comprises completing the vulnerability assessment of the workstation by a network workstation assessment service maintained on the network server, the network workstation assessment service operative to generate the workstation security credentials, wherein the workstation security policy is maintained on the workstation, the process further comprising the step of

providing the workstation security credentials from the network workstation assessment service to the workstation security policy on the workstation via the computer network;

comparing the workstation security credentials to a workstation security policy to determine whether the workstation should be granted access to the network service; and

authorizing access to the network service by the workstation if the workstation security credentials satisfy the workstation security policy, otherwise denying access to the network service by the workstation.

7. (Original) The computer-implemented process recited by Claim 1, wherein the step of generating the workstation security credentials comprises completing the vulnerability assessment of the workstation by a network workstation assessment service maintained on an assessment server coupled to the computer network, the assessment server operating as a remote server different from the network server, the network workstation assessment service operative to generate the workstation security credentials.

Application Serial No. 09/607,375

8. ((Original)) The computer-implemented process recited by Claim 7, wherein the workstation security policy is maintained on the network server, the process further comprising the steps of:

transmitting the workstation security credentials from the network workstation assessment service on the assessment server to the network service on the network server via the computer network; and

comparing at the network server the workstation security credentials to the workstation security policy to determine whether the workstation should be granted access to the network service.

9. (Original) The computer-implemented process recited by Claim 8 further comprising the step of communicating a service decision from the network server to the workstation via the computer network, the service decision defining whether the workstation is allowed to access the network service or a degraded form of the network service.

10. (Original) The computer-implemented process recited by Claim 1, wherein the step of generating the workstation security credentials comprises completing the vulnerability assessment of the workstation by the network service on the network server in response to receiving a request for the network service from the workstation via the computer network.

11. (Original) The computer-implemented process recited by Claim 10, wherein the workstation security policy is maintained on the network server, the process further comprising the step of comparing at the network server the workstation security credentials to the workstation security policy to determine whether the workstation should be granted access to the network service or a degraded form of the network service.

**[The Remainder of this page has been intentionally left blank.]**

Application Serial No. 09/607,375

12. (Currently Amended) A network security system for authenticating a workstation requesting a network service from a network server via a computer network, comprising:

a local workstation assessment service, operative on the workstation, for generating workstation security credentials by completing a vulnerability assessment of the workstation comprising a scan to identify at least one of security vulnerabilities that would compromise the secure operation of the workstation on the computer network and evidence of a compromise, the workstation security credentials comprising one of integrity information describing whether the workstation has been compromised, and security posture information describing the workstation's potential for compromise; and

a workstation security policy, operative on the workstation, for defining security policy requirements for secure operations by the workstation;

the local workstation assessment service further operative for comparing the workstation security credentials to the workstation security policy to determine whether the workstation should be granted access to the network service,

the local workstation assessment service further operative to authorize access to the network service by the workstation if the workstation security credentials satisfy the workstation security policy.

13. (Currently amended) A network security system for authenticating a workstation requesting a network service from a network server via a computer network, comprising:

a local workstation assessment service, operative on the workstation, for generating workstation security credentials by completing a vulnerability assessment comprising a scan of the workstation to identify at least one of security vulnerabilities that would compromise the secure operation of the workstation on the computer network and evidence of a compromise, the workstation security credentials comprising one of integrity information describing whether the workstation has been compromised, and security posture information describing the workstation's potential for compromise; and

a network service, operative on the network server, for determining whether the workstation should be granted access to a software service of the network service in response to receiving the workstation security credentials via the computer network.

Application Serial No. 09/607,375

14. (Original) The network security system recited by Claim 13 further comprising a workstation security policy at the network server, the workstation security policy operative to define security requirements for secure operation of the workstation on the computer network.

15. (Original) The network security system recited by Claim 14, wherein the network service is further operative for comparing the workstation security credentials to the workstation security policy to determine whether the workstation should be granted access to the software service, the network service operative to authorize access to the software service by the workstation if the workstation security credentials satisfy the workstation security policy.

**[The Remainder of this page has been intentionally left blank.]**

Application Serial No. 09/607,375

16. (Currently amended) A network security system for authenticating a workstation requesting a network service from a network server via a computer network, comprising:

the network service operative to generate workstation security credentials by completing a vulnerability assessment comprising a scan of the workstation to identify at least one of security vulnerabilities that would compromise the secure operation of the workstation on the computer network and evidence of a compromise, the workstation security credentials comprising one of integrity information describing whether the workstation has been compromised, and security posture information describing the workstation's potential for compromise;

the network service further operative to determine whether the workstation should be granted access to a software service of the network based on the workstation security credentials.

17. ((Original)) The network security system recited by Claim 16 further comprising a workstation security policy at the network server, the workstation security policy operative to define security requirements for secure operation of the workstation on the computer network.

18. (Original) The network security system recited by Claim 17, wherein the network service is further operative to compare the workstation security credentials to the workstation security policy to determine whether the workstation should be granted access to the software service, the network service operative to authorize access to the software service by the workstation if the workstation security credentials satisfy the workstation security policy.

[The Remainder of this page has been intentionally left blank.]

Application Serial No. 09/607,375

19. (Currently amended) A computer-implemented process for authenticating a workstation requesting a network service from a network server via a computer network, comprising the steps:

issuing a request for a log-in page to a network server from a browser operating on the workstation;

transmitting the log-in page and an authentication plug-in from the network server to the workstation via the computer network, the authentication plug-in installable within the browser and operative to generate workstation security credentials by completing a vulnerability assessment comprising a scan of the workstation to identify at least one of security vulnerabilities that would compromise the secure operation of the workstation on the computer network and evidence of a compromise, the workstation security credentials comprising one of integrity information describing whether the workstation has been compromised, and security posture information describing the workstation's potential for compromise;

transmitting the workstation security credentials from the authentication plug-in to the network server via the computer network; and

determining at a CGI script operating on the network server whether the workstation should be granted access to a software service of the network based on the workstation security credentials.

20. (Original) The computer-implemented process recited by Claim 19 wherein the step of determining whether the workstation should be granted access to the software service comprises the step of the CGI script comparing the workstation security credentials to a workstation security policy maintained at the network server to determine whether the workstation should be granted access to the software service;

if the workstation security credentials satisfies the workstation security policy, then authorizing access to the software service and directing the browser to the log-in page via the computer network.

otherwise, denying access to the software service and delivering an access denied page to the workstation via the computer network.

[The Remainder of this page has been intentionally left blank.]



Application Serial No. 09/607,375

21. (Currently Amended) A network security system for authenticating a workstation requesting a network service operating on a network server via a computer network, comprising:

a network assessment service operating on a network workstation assessment server on the computer network, the network assessment service operative to generate workstation security credentials prior to receiving user credentials by completing a vulnerability assessment comprising a scan of the workstation via the computer network to identify at least one of security vulnerabilities that would compromise the secure operation of the workstation on the computer network and evidence of a compromise, the workstation security credentials comprising one of integrity information describing whether the workstation has been compromised, and security posture information describing the workstation's potential for compromise,

the network service, responsive to receiving the workstation security credentials from the network assessment service via the computer, operative to determine whether the workstation should be granted access to a software service of the network based on the workstation security credentials and the user credentials.

22. (Original) The network security system recited by Claim 21 further comprising a workstation security policy at the network server, the workstation security policy operative to define security requirements for secure operation of the workstation on the computer network.

23. (Original) The network security system recited by Claim 22, wherein the network service is further operative to compare the workstation security credentials to the workstation security policy to determine whether the workstation should be granted access to the software service, the network service operative to authorize access to the software service by the workstation if the workstation security credentials and the user credentials satisfy the workstation security policy.

24. (Original) The network security system recited by Claim 21, wherein the network service is operative to transmit to the network assessment service via the computer network a request to complete the vulnerability assessment of the workstation in response to receiving a request for the software service from the workstation.

Application Serial No. 09/607,375

25. (Currently amended) A computer-implemented process for authenticating a workstation requesting a network service from a network server via a computer network, comprising the steps:

issuing a request for a log-in page to a network server from a browser operating on the workstation;

transmitting the log-in page, an authentication plug-in, and a workstation policy from the network server to the workstation via the computer network, the authentication plug-in installable within the browser and operative to generate workstation security credentials by completing a vulnerability assessment comprising a scan of the workstation to identify at least one of security vulnerabilities that would compromise the secure operation of the workstation on the computer network and evidence of a compromise, the workstation security credentials comprising one of integrity information describing whether the workstation has been compromised, and security posture information describing the workstation's potential for compromise;

comparing the workstation security credentials to the workstation policy on the workstation to determine whether the workstation should be granted access to a software service of the network; and

receiving user credentials if the workstation is granted access to the software service of the network.

[The Remainder of this page has been intentionally left blank.]